ثغرات الـ Database Disclosure بتطبيقات الـ ASP

تعد ثغرات الـ Database Disclosure ، ثغرات خطيرة نسبياً
حيث انها تعمل على تحميل ملف قاعدة بيانات التطبيق المصاب الـ Database
والأطلاع عليها من قبل المهاجم . (غالباً يحمل ملف القاعدة User pass مدير التطبيق)
الثغرات هذه تستهدف التطبيقات المبرمجة بالـ ASP بشكل خاص ،
كما من الممكن ان تواجهة تطبيقات مبرمجة بلغات اخر مع تغير مسمى الثغرة
الى Arbitrary Database Backup - Admin Backup Bypass الخ ..
انتشر هذا النوع من الثغرات بأوائل سنة ٢٠٠٧ .
سبب الثغرة يعود الى المبرمج حيث ان الثغرة عبارة عن خلل برمجي
او خطأ برمجي ان صح التعبير
يمكن الزوار من تحميل ملف داتا بيز قاعدة التطبيق والأطلاع على محتوياته !

تطبيق عملي :
اكتشفت ثغرة امنية بتطبيق asp عبارة عن منتدى اسمه iyzi Forum
وتم تسجيلها بمواقع السيكروتي
http://www.exploit-db.com/exploits/7449 ،
لحظو معي كيف تمت عملية اكتشاف الثغرة

١- قمت بتحميل التطبيق "سكربت" على جهازي من خلال موقع
التطبيق الرسمي www.iyziforum.com .

٢- قمت بفتح محتويات السكربت وجدت مجلد بأسم db وداخله ملف داتا بيز
باسم iyziforum وبصيغة mdb .

٣- قمت بفتح ملف الداتا بيز بأحد برامج المايكرسوفت اوفس فأذا ببيانات السكربت
تظهر لي ومنها user pass مدير السكربت .

٤- قمت بكتابة الاستغلال للثغرة ليخرج لي بهذا الشكل
www.xxxx.com/db/iyziforum.mdb .

وبهذا الشكل تم اكتشاف الثغرة وتسجيلها بمواقع السيكروتي بأسمي . (:

امثلة لثغرات :
http://www.exploit-db.com/exploits/7629
http://www.exploit-db.com/exploits/8878
http://www.exploit-db.com/exploits/7372
http://www.exploit-db.com/exploits/7371

انتهى .

By Ghost Hacker
My Blog : http://gh05th4ck.wordpress.com